



AD 2143
P. M. W.

PATENT
09/801,612

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: : Group Art Unit: 2143
: Examiner: A. M. Lezak
Gerald F. McBrearty et al. : Intellectual Property
Serial No: 09/801,612 : Law Department - 4054
Filed: 03/08/2001 : International Business
Title: PROTECTING CONTENTS : Machines Corporation
OF COMPUTER DATA FILES FROM : 11400 Burnet Road
SUSPECTED INTRUDERS BY : Austin, Texas 78758
RENAMING AND HIDING DATA : Customer No. 32,329
FILES SUBJECTED TO INTRUSION :
Date: 7/22/05 :

CERTIFICATE OF MAILING

I hereby certify that this correspondence including a Brief on Appeal (in triplicate), this transmittal letter (duplicate) and a check for the \$120 fee for One Month Time Extension is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450 on 7/22/05.

J. B. KRAFT

J. B. Kraft 7/22/05
Signature Date

TRANSMITTAL OF APPELLANTS' BRIEF UNDER 37 CFR 1.192(a)
AND REQUEST FOR TIME EXTENSION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Attached is Appellants' Brief (in triplicate) in this Appeal from a decision of the Examiner dated February 10,

AUS920000941US1

1

07/27/2005 WABDELRI 00000035 09801612
120.00 DP
01 FC:1251

PATENT
09/801,612

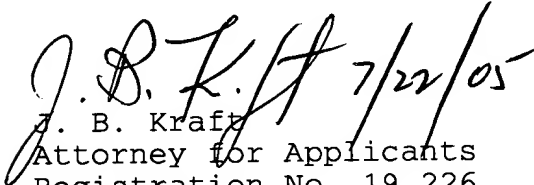
2005 finally rejecting claims 1-45.

A one month extension of time within which to file this Brief is respectfully requested. Attached is check for \$120 to cover extension fee.

Please charge our Deposit Account No. 09-0447 in the amount of \$500.00 for the Appeal Brief fee. (a duplicate of this transmittal is included.)

The Commissioner is hereby authorized to charge any additional fee which may be required or credit any overpayment to Deposit Account No. 09-0447.

Respectfully submitted,


J. B. Kraft
Attorney for Applicants
Registration No. 19,226
(512) 473-2303

PLEASE MAIL ALL CORRESPONDENCE TO:

Herman Rodriguez
IPLaw Dept. - IMAD 4054
IBM Corporation
11400 Burnet Road
Austin, Texas 78758



PATENT
09/801,612

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: : Group Art Unit: 2143
: Examiner: A. M. Lezak
Gerald F. McBrearty et al. : Intellectual Property
Serial No: 09/801,612 : Law Department - 4054
Filed: 03/08/2001 : International Business
Title: PROTECTING CONTENTS : Machines Corporation
OF COMPUTER DATA FILES FROM : 11400 Burnet Road
SUSPECTED INTRUDERS BY : Austin, Texas 78758
RENAMING AND HIDING DATA : Customer No. 32,329
FILES SUBJECTED TO INTRUSION :
Date: 7/22/05 :

BRIEF ON APPEAL

Commissioner for Patents
P.O.Box 1450
Alexandria, VA 22313-1450

Sir:

This is an Appeal from the Final Rejection of Claims 1-45 of this Application dated February 10, 2005. VIII. Appendix containing a copy of each of the Claims is attached.

I. Real Party in Interest

The real party in interest is International Business Machines Corporation, the assignee of the present Application.

II. Related Appeals and Interferences

None

III. Status of Claims

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

There are 45 claims in this Application.

B. STATUS OF ALL THE CLAIMS

1. Claims cancelled: None.
2. Claims withdrawn from consideration but not cancelled: None.
3. Claims pending: 1-45.
4. Claims allowed: None.
5. Claims rejected: 1-45.

C. CLAIMS ON APPEAL

Claims on appeal: 1-45.

IV Status of Amendments

No amendments have been filed after Final Rejection.

V. Summary of Claimed Invention

In a data processing operation having stored data in a plurality of data files, the present invention (as defined in independent claims 1, 16, and 31) provides an implementation for protecting the data files from unauthorized users comprising means for receiving user requests for access to data files (referring to Fig. 1 of drawings, the present Specification, page 7 lines 30-33 describes requests from IP locations 63 and 65 made to Web station 57 which controls a database including directory 55 containing groups of files 58, 59...68, 69, p.7, lines 18-21); means for determining whether the requests are unauthorized intrusions into the requested data files (referring to Fig. 1, page 8, lines 6-9 describe file requests being authenticated within firewall section 52 of server 53 using Kerberos protocols); and means, responsive to a determination that a request is an unauthorized intrusion, for changing the identification of the requested data files (page 9, lines 2-9, still referring to Fig. 1, describes a determination that authentication of requests for files 58 and 59 has been unsuccessful. This failure triggers an alert which in turn causes file 59, for example, to be renamed file 72).

Independent claims 8, 23, and 38 cover the above described invention in a network environment. Fig. 1 as described by the above mentioned sections in the Specification describing the implementation being carried on the World Wide Web network.

VI. Grounds of Rejection

Claims 1-45 are rejected under 35 USC 103(a) as unpatentable over Schneck et al. (US5,933,498) in view of the Margolus et al. Publication (US2002/0038296).

VII. Argument

Claims 1-45 are unobvious over the combination of Schneck et al. (US5,933,498) in view of the Margolus Publication (US2002/0038296), and, therefore, are patentable under 35 USC 103(a).

The basic Schneck reference fails to even suggest the key to the present invention: changing the identification of requested data files responsive to determination that request is an unauthorized intrusion.

Applicants concur with Examiner that Schneck discloses determining whether received requests for data files, in a network environment, are unauthorized. Applicants also concur with Examiner's conclusion that: Schenk does not teach means, responsive to unauthorized intrusion, for changing identification of requested data files (page 3, paragraph 4 of the Final Rejection herein).

However, Applicants disagree with Examiner's position that there is a suggestion in Schneck that its teaching could be modifiable to disclose the present invention. The Examiner points to columns 7 and 8 in Schneck as suggesting such a modification. This portion of Schneck and subsequent portions set forth elaborate sets of rules for first determining the type of intrusion, and then providing an expedient for responding to the intrusion. While Schneck's responses include destruction or encryption of invaded files, there is no suggestion whatsoever of changing the identification of the intruded files.

This omission becomes even more significant when one considers that in the whole comprehensive description in Schneck et al. (34 columns and 26 sheets of drawings) covering rules for protecting data, there is no hint whatsoever of changing the identification of the data file subjected to the unauthorized request.

The Margolus Publication fails to make up for the failure of Schneck to teach changing identification of the intruded upon data files.

Since Schneck does not even suggest how it would modifiable to disclose the present invention of renaming intruded upon files, the proposed modification must be clearly disclosed by Margolus in order to reasonably provide any basis for combining the references. Margolus fails to do this.

For this teaching in Margolus, Examiner cites 10 continuous columns (paragraphs 0011-0032) as well as paragraphs 55 and 62 and claims 1-153. Applicants have reviewed these sections and claims, and still fail to find any suggestion of changing the identification or name of any file responsive to an unauthorized intrusion. The descriptive material above cited in Margolus does describe changing names when new versions of objects are created but this does not seem to have anything to do with unauthorized intrusions.

The Examiner more specifically points to paragraph 0011 and claims 18-26 teaching the need for access authorization to a named object, the contents of which determine the location of the data in the storage device. The Examiner makes the assumption that the contents may be changed to point to the location of another file, e.g. a backup file. Applicants fail to understand how this is a teaching of

responding to an unauthorized intrusion request by changing the identity of the requested file. If the Examiner has a logical rationale for her conclusion, Applicants would appreciate the Examiner specifying her position in her Answer so that Applicants may respond in their Reply Brief.

The Examiner argues (Section 5. of Final Rejection) that it would have been obvious to incorporate the backup/replacement means of Margolus in the Schneck system. Applicants still fail to see how such a combination even if made would disclose responding to an unauthorized intrusion request by changing the identity of the requested file.

The Examiner's proposed combinations of elements from the Schneck and Margolus references in the rejection is being offered without requisite foresight but only in light of Applicants' own teaching.

In combining the Schneck and Margolus references, the Examiner has picked and chosen elements from each reference not in the light of teachings from the references but in the light of Applicants' own teaching. Thus it is submitted that Examiner's proposed combination of references is being made not with the requisite foresight of one skilled in the art, but rather with the hindsight obtained solely by the teaching of the present invention. This approach cannot be used to render Applicants' invention unpatentable.

"To imbue one of ordinary skill in the art with knowledge of the invention in suit, when no prior art references of record convey nor suggest that knowledge, is to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher." W. L. Gore, 721 F 2d at 1553, 220 USPQ, pp. 312-313.

"One cannot use hindsight reconstruction to pick and choose among isolated disclosures in the

prior art to deprecate the claimed invention." In re Fine, 5 USPQ 2d 1596 (C.A.F.C.) 1988.

However, it is further submitted that even if the elements from the two references are selected and combined as suggested by Examiner, the combination would still fail to teach responding to an unauthorized intrusion request by changing the identity of the requested file. The Examiner admits that the basic Schneck fails to teach this element. The modifying Margolus reference also fails to teach responding to unauthorized intrusion by changing identity of requested file. Margolus chnges identity when new versions of objects are created but not upon unauthorized intrusion.

Claims 2-4, 9-11, 17-19, 24-26, 32-34, and 39-41 are more specifically patentable over the combination of Schneck and Margolus.

These dependent claims are submitted to be patentable over the combination of references for the reasons set forth above for the patentability of the independent claims from which the present claims respectively depend. In addition, these claims set forth that the change in identification is achieved by changing the file indentifiers or file names in response to an unauthorized intrusion request. Applicants have carefully considered the references and found that the times that Margolus reference changes identifiers or names are when new versions of the files are created. Applicants have not found anything in either reference which changes a file name or identifier in response to any kind of unauthorized intrusion request.

Claims 5, 12, 20, 27, 35, and 42 are more specifically patentable over the combination of Scneck and Margolus.

These dependent claims are submitted to be patentable over

the combination of references for the reasons set forth above for the patentability of the independent claims from which the present claims respectively depend. In addition, these claims set forth a new directory for tracking renamed files. It appears that Margolus does disclose listing of files in directories. This still does not change the basic patentability of the present claims in that the two references still do not teach changing a file name or identifier in response to any kind of unauthorized intrusion request.

Claims 6, 7, 13, 14, 21, 22, 28, 29, 36, 37, 43 and 44 are more specifically patentable over the combination of Scneck and Margolus.

These dependent claims are submitted to be patentable over the combination of references for the reasons set forth above for the patentability of the independent claims from which the present claims respectively depend. In addition, these claims set forth assigning a covert name indicating a covert location in a new directory. For this teaching, the Examiner points to disclosures in Margolus of encryption and decryption. It is not necessary to argue whether this encryption-decryption is equivalent to Applicants' covert names. Applicants simply take the position that irrespective of whether Margolus discloses renaming files with covert names for any purpose, the combination of references simply fails to disclose changing a file name or identifier in response to any kind of unauthorized intrusion request.

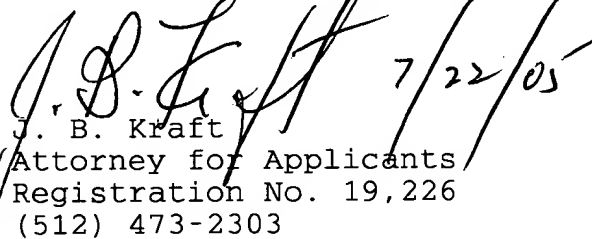
PATENT
09/801,612

Conclusion

In view of the foregoing, it is submitted that Claims 1-45 are unobvious over the combination of Schneck et al. (US5,933,498) in view of the Margolus Publication (US2002/0038296), and, therefore, are patentable under 35 USC 103(a).

Therefore, it is respectfully requested that the Final Rejection of claims 1-45 dated February 10, 2005 be reversed, and that claims 1-45 be found to be in condition for allowance.

Respectfully submitted,

 7/22/05
J. B. Kraft
Attorney for Applicants
Registration No. 19,226
(512) 473-2303

PLEASE MAIL ALL CORRESPONDENCE TO:

Herman Rodriguez
IPLaw Dept. - IMAD 4054
IBM Corporation
11400 Burnet Road
Austin, Texas 78758

VIII. Claims Appendix

1 1. In a data processing operation having stored data in a
2 plurality of data files, a system for protecting said data
3 files from unauthorized users comprising:
4 means for receiving user requests for access to data
5 files;
6 means for determining whether said requests are
7 unauthorized intrusions into said requested data files; and
8 means, responsive to a determination that a request is
9 an unauthorized intrusion, for changing the identification
10 of the requested data files.

1 2. The data processing operation system of claim 1 wherein
2 said means for changing the identification of said requested
3 data files change the overt identification of the requested
4 files.

1 3. The data processing operation system of claim 2 wherein
2 said means for changing the overt identification of said
3 requested data files rename said files.

1 4. The data processing operation system of claim 3 wherein
2 said file renames do not indicate the contents of the
3 renamed files.

1 5. The data processing operation system of claim 4 further
2 including means for moving said renamed files into a new
3 directory.

1 6. The data processing operation system of claim 5 further
2 including means for assigning to each of the renamed files a
3 covert name indicating a covert location in said new
4 directory for each of said renamed files.

1 7. The data processing operation system of claim 6 further
2 including a log referencing each renamed file to the covert
3 name of the respective file so as to indicate the covert
4 location of said file in said new directory.

1 8. In a communication network with access to a plurality of
2 network sites each having stored data in a plurality of data
3 files accessible in response to requests from users at other
4 sites in the network, a system for protecting said network
5 site data files from unauthorized users comprising:
6 means associated with a network site for
7 receiving user requests for access to data files;
8 means associated with said network site for determining
9 whether said user requests are unauthorized intrusions into
10 said requested data files; and
11 means associated with said network site responsive to a
12 determination that a request is unauthorized for changing
13 the identification of the requested data files.

1 9. The communication network system of claim 8 wherein said
2 means for changing the identification of said requested data
3 files change the overt identification of the requested
4 files.

1 10. The communication network system of claim 9 wherein
2 said means for changing the overt identification of said
3 requested data files rename said files.

1 11. The communication network system of claim 10 wherein
2 said file renames do not indicate the contents of the
3 renamed files.

1 12. The communication network system of claim 11 further
2 including means for moving said renamed files into a new
3 directory.

1 13. The communication network system of claim 12 further
2 including means for assigning to each of the renamed files a
3 covert name indicating a covert location in said new
4 directory for each of said renamed files.

1 14. The communication network system of claim 13 further
2 including a log referencing each renamed file to the covert
3 name of the respective file so as to indicate the covert
4 location of said file in said new directory.

1 15. The communication network system of claim 8 wherein
2 said network is the World Wide Web, and said network sites
3 are Web sites.

1 16. In a data processing operation having stored data in a
2 plurality of data files, a method for protecting said data
3 files from unauthorized users comprising:
4 receiving user requests for access to data files;
5 determining whether said requests are unauthorized
6 intrusions into said requested data files; and
7 changing the identification of the requested data files
8 responsive to a determination that a request is
9 unauthorized.

1 17. The data processing method of claim 16 wherein said
2 step of changing the identification of said requested data
3 files changes the overt identification of the requested
4 files.

1 18. The data processing method of claim 17 wherein said
2 step of changing the overt identification of said requested
3 data files renames said files.

1 19. The data processing method of claim 18 wherein said
2 file renames do not indicate the contents of the renamed
3 files.

1 20. The data processing method of claim 19 further
2 including the step of moving said renamed files into a new
3 directory.

1 21. The data processing method of claim 20 further
2 including the step of assigning to each of the renamed files
3 a covert name indicating a covert location in said new
4 directory for each of said renamed files.

1 22. The data processing method of claim 21 further
2 including the step of forming a log referencing each renamed
3 file to the covert name of the respective file so as to
4 indicate the covert location of said file in said new
5 directory.

1 23. In a communication network with access to a plurality
2 of network sites each having stored data in a plurality of
3 data files accessible in response to requests from users at
4 other sites in the network, a method for protecting said
5 network site data files from unauthorized users comprising:
6 receiving user requests for access to data files at a
7 network site;
8 determining at said network site whether said user
9 requests are unauthorized intrusions into said requested
10 data files; and
11 changing the identification of the requested data files
12 responsive to a determination that a request is
13 unauthorized.

1 24. The communication network method of claim 23 wherein
2 said step of changing the identification of said requested
3 data files changes the overt identification of the requested
4 files.

1 25. The communication network method of claim 24 wherein
2 said step of changing the overt identification of said
3 requested data files renames said files.

1 26. The communication network method of claim 25 wherein
2 said file renames do not indicate the contents of the
3 renamed files.

1 27. The communication network method of claim 26 further
2 including the step of moving said renamed files into a new
3 directory.

1 28. The communication network method of claim 27 further
2 including the step of assigning to each of the renamed files
3 a covert name indicating a covert location in said new
4 directory for each of said renamed files.

1 29. The communication network method of claim 28 further
2 including the step of forming a log referencing each renamed
3 file to the covert name of the respective file so as to
4 indicate the covert location of said file in said new
5 directory.

1 30. The communication network method of claim 23 wherein
2 said network is the World Wide Web, and said network sites
3 are Web sites.

1 31. A computer program having code recorded on a computer
2 readable medium for protecting data files from unauthorized
3 users in a data processing operation having stored data in a
4 plurality of data files, said program comprising:
5 means for receiving user requests for access to data
6 files;
7 means for determining whether said requests are
8 unauthorized intrusions into said requested data files; and
9 means responsive to a determination that a request is
10 unauthorized for changing the identification of the
11 requested data files.

PATENT
09/801,612

1 32. The computer program of claim 31 wherein said means for
2 changing the identification of said requested data files
3 change the overt identification of the requested files.

1 33. The computer program of claim 32 wherein said means for
2 changing the overt identification of said requested data
3 files rename said files.

1 34. The computer program of claim 33 wherein said file
2 renames do not indicate the contents of the renamed files.

1 35. The computer program of claim 34 further including
2 means for moving said renamed files into a new directory.

1 36. The computer program of claim 35 further including
2 means for assigning to each of the renamed files a covert
3 name indicating a covert location in said new directory for
4 each of said renamed files.

1 37. The computer program of claim 36 further including a
2 log referencing each renamed file to the covert name of the
3 respective file so as to indicate the covert location of
4 said file in said new directory.

1 38. A computer program having code recorded on a computer
2 readable medium for protecting data files from unauthorized
3 users in a communication network with access to a plurality
4 of network sites each having stored data in a plurality of
5 data files accessible in response to requests from users at
6 other sites in the network, said program comprising:
7 means associated with a network site for
8 receiving user requests for access to data files;
9 means at said network site for determining whether said
10 user requests are unauthorized intrusions into said
11 requested data files; and
12 means associated with said network site responsive to a
13 determination that a request is unauthorized for changing
14 the identification of the requested data files.

1 39. The computer program of claim 38 wherein said means for
2 changing the identification of said requested data files
3 change the overt identification of the requested files.

1 40. The computer program of claim 39 wherein said means for
2 changing the overt identification of said requested data
3 files rename said files.

1 41. The computer program of claim 40 wherein said file
2 renames do not indicate the contents of the renamed files.

1 42. The computer program of claim 41 further including
2 means for moving said renamed files into a new directory.

1 43. The computer program of claim 42 further including
2 means for assigning to each of the renamed files a covert
3 name indicating a covert location in said new directory for
4 each of said renamed files.

PATENT
09/801,612

1 44. The computer program of claim 43 further including a
2 log referencing each renamed file to the covert name of the
3 respective file so as to indicate the covert location of
4 said file in said new directory.

1 45. The computer program of claim 38 wherein said network
2 is the World Wide Web, and said network sites are Web sites.